Représentations complexes de groupes finis

Friedrich Wagemann
Université de Nantes

July 5, 2017

Introduction

Le but de parler de représentations de groupes finis en agrégation est de laisser interagir deux parties de vos connaissances en algèbre. D'une part, il s'agit d'algèbre linéaire, puisque une représentation d'un groupe G sur un espace vectoriel V est un ensemble de matrices dans $\mathrm{Gl}(V)$. Il y a une telle matrice $\rho(g)$ pour chaque élément $g \in G$. Dans notre cadre de théorie des représentations, ce sont des matrices dans $\mathrm{Gl}(V)$ sur un espace vectoriel complexe $\mathbb{C}$. Puisque dans notre cadre le groupe G est fini, ces matrices sont toutes solutions de l'équation $X^N = 1$, où N est l'ordre du groupe $N = |G|$. Ainsi ces matrices sont diagonalisables (mais pas forcément de manière simultanée), avec comme valeurs propres des racines N-èmes de l'unité.

D'une autre part, il s'agit des propriétés de groupes finis G qui se refléteront dans la représentation. Ainsi les résultats sur la théorie des groupes finis, leurs propriétés algébriques et leurs utilisation géométrique, joueront un rôle dans la théorie des représentations. C'est une bonne manière de revoir et d'approfondir vos connaissances sur les groupes symétriques, les groupes diédraux, les groupes de Klein et quaternonien, mais aussi vos connaissances sur l'action d'un groupe sur un ensemble, le produit semidirect etc. Il s'agit essentiellement de réinterpréter ces résultats de théorie des groupes et d'algèbre linéaire dans ce nouveau cadre.

Dans un premier temps, il sera question de décomposer une représentation en sous-représentations, afin d'isoler les *représentations irréductibles* comme briques élémentaires à partir desquelles toutes les représentations (complexes de dimension finie, d'un groupe fini) seront assemblées. Pour cela on utilise que les matrices $\rho(g)$ sont semisimples, i.e. tout sous-espace $\rho(g)$-stable admet un supplémentaire $\rho(g)$-stable.

La nouvelle partie de la théorie sera celle des *caractères* de groupes. Il s'agit essentiellement des fonctions $G \to \mathbb{C}$ qui s'obtiennent en tant que traces des matrices $\rho(g)$. Ces caractères sont constantes sur les classes de conjugaison du groupe G, et ce sont donc des *fonctions de classes*, d'où un lien fort entre structure du groupe (partition en classes de conjugaison) et représentations via le caractère. Le théorème principal de cette partie est que les caractères de représentations irréductibles forment une base orthonormée dans l'ensemble des fonctions de classe. Cela permettra entre autres à compléter une connaissance incomplète de la table des caractères d'un groupe.

1 Définition et exemples

Définition 1
Soit G un groupe fini et V un espace vectoriel complexe de dimension finie.

1. Une *représentation* de G sur V (ou une structure de G-*module* sur V) est un homomorphisme de groupes $\rho : G \to \mathrm{Gl}(V)$. Plus explicitement, pour tout $g, h \in G$, on a

$$\rho(gh) = \rho(g)\rho(h), \quad \rho(1) = \mathrm{id_V}.$$

   On note $\rho(g)(v)$ aussi $g \cdot v$ pour tout $v \in V$ et tout $g \in G$.

2. Pour deux représentations V et W de G, on dit que $f : V \to W$, linéaire, est un G-*morphisme* si pour tout $g \in G$,

$$f(g \cdot v) \;=\; g \cdot f(v), \quad \forall\, v \in V.$$

3. Un sous-espace vectoriel $W \subset V$, V un G-module, est appelé *sous-G-module* si

$$\forall\, g \in G, \;\; \forall w \in W : \;\; g \cdot w \in W.$$

Exemples 1

1. La *représentation triviale.* Il s'agit de l'homomorphisme $\rho : G \to \mathrm{Gl}(V)$, $g \mapsto \mathrm{id_V}$ pour tout $g \in G$.

2. Soit X un ensemble fini, muni d'une action d'un groupe fini G, i.e. pour tout $g \in G$, il existe une bijection $b_g : X \to X$ avec $b_1 = \mathrm{id_V}$ et $b_g \circ b_h = b_{gh}$. On note $b_g(x)$ aussi gx pour tout $x \in X$ et tout $g \in G$.

   On lui associe la *représentation de permutation* sur l'espace vectoriel $V := \bigoplus_{x \in X} \mathbb{C}\, e_x$, l'espace vectoriel engendré par X. G agit sur V (i.e. V devient un G-module) par

$$g \cdot e_x \;:=\; e_{gx} \;:=\; e_{b_g(x)}, \;\; \forall x \in X, \;\; \forall g \in G.$$

3. Faisons un cas spécial explicit de cette dernière construction : le groupe symétrique S_3 agit sur l'ensemble $X = \{1, 2, 3\}$. Par ce qui précède, S_3 agit sur $\mathbb{C}^3$ par permutation des vecteurs de base canoniques (e_1, e_2, e_3). $U := \mathbb{C}(e_1 + e_2 + e_3)$ est un sous-S_3-module de V qui s'identifie à la représentation triviale. W admet comme supplémentaire $V := \{ae_1 + be_2 + ce_3 \,|\, a + b + c = 0\}$. V s'appelle la *représentation standard* de S_3.

4. Faisons un autre cas spécial : G agit par *translation à gauche* sur l'ensemble G : pour tout $g \in G$, g agit par $h \mapsto gh$. Par ce qui précède, G agit sur $V := \mathbb{C}(G) := \bigoplus_{g \in G} \mathbb{C} e_g$.

Lemme 1 *Soit $f : V \to W$ un G-morphisme (sous-entendu, V et W sont des G-modules).*

Alors $\ker(f) \subset V$ *et* $\mathrm{im}(f) \subset W$ *sont des sous-G-modules.*

Démonstration. Pour tout $v \in \ker(f)$ et tout $g \in G$, on a:

$$f(g \cdot v) \;=\; g \cdot f(v) \;=\; g \cdot 0 \;=\; 0,$$

donc $g \cdot v \in \ker(f)$.

Pour tout $w \in \mathrm{im}(f)$, il existe $v \in V$ tel que $f(v) = w$. D'où, pour tout $g \in G$:

$$g \cdot w \;=\; g \cdot f(v) \;=\; f(g \cdot v) \;\in\; \mathrm{im}(f).$$

□

2 Irréductibilité et Lemme de Schur

Définition 2
Une représentation V s'appelle *irréductible* (on dit aussi que le G-module V est *simple*) si les seuls sous-G-modules de V sont $\{0\}$ et V lui-même.

Proposition 1 *Soit $W \subset V$ un sous-G-module, G groupe fini. Alors il existe un supplémentaire G-stable, i.e. il existe $W' \subset V$ sous-G-module avec*

$$V \;=\; W \oplus W'.$$

Remarque 1
Le théorème de Maschke affirme que ceci reste vrai en caractéristique p pourvu que p ne divise pas l'ordre du groupe $|G|$. (On remarque que la deuxième démonstration marche dans ce cadre plus général.)

Démonstration. Il y a (au moins) deux manières de montrer cela:

1. Soit H_0 un produit Hermitien sur V. On rend H_0 un produit Hermitien G-invariant :

   $$H(v,w) \;:=\; \sum_{g \in G} H_0(g \cdot v, g \cdot w)$$

   pour tout $v, w \in V$. Alors H est bien G-invariant: pour tout $g \in G$,

   $$\begin{aligned} H(g \cdot v, g \cdot w) &= \sum_{h \in G} H_0(gh \cdot v, gh \cdot w) \\ &= \sum_{k \in G} H_0(k \cdot v, k \cdot w) \;=\; H(v,w). \end{aligned}$$

Soit maintenant $W' := W^{\perp_H} := \{v \in V \,|\, \forall w \in W : \, H(v,w) = 0\}$. Alors W' est G-invariant : pour tout $g \in G$, $v \in W'$, $w \in W$:

$$\begin{aligned} H(g \cdot v, w) &= H(g \cdot v, gg^{-1} \cdot w) \\ &= H(v, g^{-1} \cdot w) = 0, \end{aligned}$$

car $v \in W^{\perp_H}$ et $g^{-1} \cdot w \in W$. Par ailleurs, $V = W \oplus W'$.

2. Soit W'' un sous-espace de V avec $V = W \oplus W''$ et $\pi_0 : V \to W$ la projection associée à cette décomposition. On rend π_0 G-équivariant (i.e. un G-morphisme) comme suit : pour tout $v \in V$:

$$\pi(v) := \sum_{g \in G} g \cdot \pi_0(g^{-1} \cdot v).$$

Alors π est un G-morphisme de V sur W: pour tout $h \in G$ et tout $v \in V$:

$$\begin{aligned} \pi(h \cdot v) &= \sum_{g \in G} g \cdot \pi_0(g^{-1}h \cdot v) \\ &= \sum_{k \in G} hk \cdot \pi_0(k^{-1} \cdot v) \; = \; h \cdot \pi(v), \end{aligned}$$

où on a posé $k := h^{-1}g$ pour faire un changement d'indexation.

Le restriction de π à W s'identifie à la multiplication par l'entier $|G|$. $W' := \ker(\pi)$ est un sous-G-module de V avec $V = W \oplus W'$.

En effet, si $w \in W \cap W'$, alors $\pi(w) = 0$ et $\pi(w) = |G|w$, donc $w = 0$. Enfin, $\mathrm{im}(\pi) = W$. En effet, puisque la restriction de π à W est la multiplication par l'entier $|G|$, $W \subset \mathrm{im}(\pi)$. Réciproquement, si $w \in \mathrm{im}(\pi)$, on a $w = \sum_{g \in G} g \cdot \pi_0(g^{-1} \cdot v) \in W$, car $\pi_0(g^{-1} \cdot v) \in W$.

□

Corollaire 1 *Toute représentation est la somme directe de représentations irréductibles.*

Remarque 2
Cette propriété s'appelle *réductibilité complète* ou *semi-simplicité*. En fait, si l'on passe à des groupes plus généraux que les groupes finis, les groupes *compacts* ont cette propriété. Dans ce cas, c'est l'intégration sur G qui remplace la somme sur les éléments de G dans la moyenne qui intervient dans la démonstration précédente.

Le groupe abélien $\mathbb{R}$ n'a pas cette propriété: la représentation

$$\mathbb{R} \ni a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in \mathrm{End}(V) = M_2(\mathbb{C})$$

possède $\mathbb{C}e_1$ comme sous-espace stable, mais il n'a pas de supplémentaire stable.

Sinon, en caractéristique p (on parle de *représentations modulaires*), cette propriété peut aussi faire défaut.

Lemme 2 (Lemme de Schur) *Soient V, W deux G-représentations irréductibles, $f : V \to W$ un G-morphisme. Alors*

1. *Soit f est un isomorphisme, soit $f = 0$.*
2. *Si $V = W$, alors $f = \lambda \mathrm{id}_{\mathrm{v}}$ pour un $\lambda \in \mathbb{C}$.*

Démonstration.

1. Puisque $\ker(f)$ et $\mathrm{im}(f)$ sont des sous-G-modules (Lemme 1) et V et W sont irréductibles, on a les deux choix suivants : soit $\ker(f) = 0$ et $\mathrm{im}(f) = W$, i.e. f est un isomorphisme, soit $\ker(f) = V$ et $\mathrm{im}(f) = 0$, i.e. $f = 0$.
2. Sur $\mathbb{C}$, $f : V \to V$ possède une valeur propre (c'est exactement pour cela que nous n'étudions que les représentations *complexes* !) $\lambda \in \mathbb{C}$. Alors $f - \lambda \mathrm{id}_{\mathrm{V}}$ est un G-morphisme ayant un noyau non-trivial. Par irréductibilité, on a donc $\ker(f - \lambda \mathrm{id}_{\mathrm{V}}) = \mathrm{V}$, i.e. $f = \lambda \mathrm{id}_{\mathrm{V}}$.

□

Théorème 1 *Soit V une représentation (de dimension finie) d'un groupe fini G. Alors il existe une décomposition*

$$V \;=\; V_1^{\oplus a_1} \oplus \ldots \oplus V_k^{\oplus a_k},$$

où les V_i sont des représentations irréductibles distinctes. De plus, la décomposition est unique dans le sens où les V_i sont uniques à isomorphisme près, et les multiplicités *a_i sont uniques.*

Démonstration. L'existence est assurée par le Corollaire 1. L'unicité se déduit du Lemme de Schur : si $W = W_1^{\oplus b_1} \oplus \ldots \oplus W_k^{\oplus b_k}$ est un autre G-module et $f : V \to W$ un G-morphisme, alors f envoie le facteur $V_i^{\oplus a_i}$ sur le facteur $W_j^{\oplus b_j}$ avec $W_j \cong V_i$. S'il n'y a pas de tel facteur, $f = 0$. (En effet, on applique le Lemme de Schur à la restriction de f à un certain facteur V_i, composée avec la projection sur un facteur W_j. Le lemme dit alors que c'est un isomorphisme ou nul.)

Si on applique cela à l'identité id_{V} avec deux décompositions différentes de V, on obtient l'unicité des V_i et des a_i. □

3 Représentations de groupes abéliens

Dans cette section, G désigne un groupe abélien qui n'est pas nécessairement fini.

Lemme 3 *Une représentation irréductible V de G est nécessairement de dimension* 1.

Démonstration. observation : puisque G est abélien, les éléments de G donnent des G-morphismes $g : V \to V$. En effet, pour tout $h \in G$ et tout $v \in V$, on a

$$h \cdot (g \cdot v) \;=\; (hg) \cdot v \;=\; (gh) \cdot v \;=\; g \cdot (h \cdot v).$$

Par le Lemme de Schur, $g : V \to V$ s'identifie à $\lambda_g \mathrm{id_V}$. Mais alors, si $\dim(V) \neq 1$, V aurait des sous-G-espaces non réduits à $\{0\}$ ou V, ce qui contredit l'irréductibilité de V. $\square$

Définition 3
Soit G un groupe abélien. On appelle l'ensemble

$$\widehat{G} \;:=\; \mathrm{Hom}(G, S^1)$$

le *groupe dual* (ou le *dual de Pontryagin*) de G. Ici, $S^1 = \mathbb{R}/2\pi\mathbb{Z}$ désigne le cercle unité, vu comme groupe abélien.

Remarque 3
Si G est un groupe topologique non-discret, on demande en plus que les homomorphismes soient continus. Si G est abélien compact ou abélien fini, alors

$$\mathrm{Hom}_{\mathrm{cont}}(G, S^1) = \mathrm{Hom}_{\mathrm{cont}}(G, \mathbb{C}^*).$$

En effet, si $f \in \mathrm{Hom}_{\mathrm{cont}}(G, \mathbb{C}^*)$, $f(g^n) = f(g)^n$ doit être borné, car $f(G) \subset \mathbb{C}^*$ est compact.

Exemples 2

1. $G = \mathbb{Z}$: $\mathrm{Hom}(\mathbb{Z}, S^1) \cong S^1$.
2. $G = S^1$: $\mathrm{Hom}_{\mathrm{cont}}(S^1, S^1) \cong \mathbb{Z}$, d'après la proposition ci-dessous :

   Proposition 2 *Les* $e_n(x) \;:=\; e^{2\pi i n x}$ *forment un système complet, pour* $n \in \mathbb{Z}$*, d'éléments de* $\widehat{S^1}$*.*

   Démonstration. On a bien $e_n(x + y) = e_n(x)e_n(y)$, donc $e_n \in \widehat{S^1}$.

   Un élément quelconque e de $\widehat{S^1}$ vérifie $e(x) = e^{i\phi(x)}$. Or, e est un homomorphisme, donc ϕ est additive modulo 2π. $\phi(nx) = n\phi(x)$ modulo 2π pour tout $n \in \mathbb{Z}$ implique $\phi(x) = x\phi(1)$ modulo 2π pour tout $x \in \mathbb{Q}$. Par continuité, on en conclut $e(x) = e^{ix\phi(1)}$ pour tout $x \in \mathbb{R}$. Or,

   $$1 \;=\; e(0) \;=\; e(1) \;=\; e^{\phi(1)},$$

   et ainsi il existe $n \in \mathbb{Z}$ avec $\phi(1) = 2\pi n$. $\square$

Corollaire 2

$$\widehat{\widehat{S^1}} \cong S^1.$$

Remarque 4
La théorie de la dualité de Pontryagin montre que le dual d'un groupe abélien compact est un groupe abélien discret, et que le dual d'un groupe abélien discret est un groupe abélien compact. Le théorème principal de Pontryagin montre pour de tels groupes G que $\widehat{\widehat{G}} \cong G$.

3. $G = \mathbb{Z}_m$ $(= \mathbb{Z}/m\mathbb{Z})$: $\mathrm{Hom}(\mathbb{Z}_m, S^1) \cong \mathbb{Z}_m$.

   Démonstration. $\mathbb{Z}_m$ est isomorphe à $\frac{2\pi}{m}\mathbb{Z}/2\pi\mathbb{Z} \subset \mathbb{R}/2\pi\mathbb{Z}$ par l'isomorphisme $\phi : k + m\mathbb{Z} \mapsto \frac{2\pi k}{m} + 2\pi\mathbb{Z}$. D'où un homomorphisme injectif $\Phi : \mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_m) \to \mathrm{Hom}(\mathbb{Z}_m, S^1)$, $f \mapsto f \circ \phi$.

   Pour $g \in \mathrm{Hom}(\mathbb{Z}_m, S^1)$, $g(\mathbb{Z}_m) \subset \frac{2\pi}{m}\mathbb{Z}/2\pi\mathbb{Z}$, et $f = \phi^{-1} \circ g \in \mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_m)$. Donc Φ est un isomorphisme. Or, par ailleurs, $\mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_m) \cong \mathbb{Z}_m$. $\square$

Remarque 5
Tout groupe abélien de type fini est de la forme $\mathbb{Z}^n \oplus \bigoplus_{i=1}^{l} \mathbb{Z}_{m_i}$, un groupe abélien *fini* est donc une somme directe de tels $\mathbb{Z}_{m_i}$. La prise du dual de Pontryagin se comporte bien par rapport à la somme directe de groupes abéliens.

4. $G = \mathbb{R}$: $\mathrm{Hom}_{\mathrm{cont}}(\mathbb{R}, S^1) \cong \mathbb{R}$.

   La démonstration est ici la même que celle pour $G = S^1$, sauf qu'il n'y a pas de restriction sur $\phi(1)$.

4 Transformée de Fourier sur les groupes abéliens

Le fil conducteur de cette section est que pour toute paire de duaux de Pontryagin $(G, \widehat{G})$, on a une transformée de Fourier, exactement de la même façon que pour la transformée de Fourier usuelle qui est associée à la paire $(S^1, \mathbb{Z})$.

Rappelons la transformée de Fourier pour la paire $(S^1, \mathbb{Z})$. Pour cela, on regarde les fonctions $f \in L^2(S^1)$ comme fonctions $f : \mathbb{R} \to \mathbb{C}$ avec $f(x+1) = f(x)$ pour tout $x \in \mathbb{R}$. L'espace $L^2(S^1)$ est alors l'espace des f tels que

$$||f||_2 := \left(\int_0^1 |f|^2 \right)^{\frac{1}{2}} < \infty.$$

C'est un espace de Hilbert avec le produit Hermitien

$$(f, g) := \int_0^1 f \, \bar{g}.$$

Théorème 2 *Les fonctions* $e_n(x) = e^{2\pi inx}$, $n \in \mathbb{Z}$, *forment une base (de Hilbert) orthonormale de* $L^2(S^1)$ *dans le sens où*

$$\forall f \in L^2(S^1): \quad f = \sum_{n=-\infty}^{\infty} \hat{f}(n) e_n$$

avec

$$\hat{f}(n) := (f, e_n) = \int_0^1 f(x) e^{-2\pi inx} dx.$$

Ceci fournit un isomorphisme d'espaces de Hilbert

$$L^2(S^1) \to l^2(\mathbb{Z}), \;\; f \mapsto \hat{f},$$

et on a l'identité de Plancherel

$$||f||_2^2 = \int_0^2 |f|^2 = \sum_{n=-\infty}^{\infty} |\hat{f}(n)|^2.$$

De plus, si l'on munit $L^1(S^1)$ *du* produit de convolution

$$f * g := \int_0^1 f(x-y) g(y) dy,$$

alors le produit de convolution est associatif et commutatif. $L^2(S^1) \subset L^1(S^1)$ *est un idéal pour le produit de convolution et on a:*

$$\widehat{(f * g)} = \hat{f}\hat{g}.$$

On peut énoncer des théorèmes de ce type pour toute paire de groupes duaux de Pontryagin. C'est un des objectifs de *l'analyse harmonique* de démontrer ce type de théorème. Les éléments du groupe dual $\hat{G}$ sont aussi appelés les *caractères* du groupe G. Nous allons nous contenter ici de la paire $(\mathbb{Z}_m, \mathbb{Z}_m)$ qui nous emmène à la *transformée de Fourier discrète.*

La dualité $\widehat{\mathbb{Z}_m} \cong \mathbb{Z}_m$ se voit grâce aux exponentielles

$$e(l) = e^{2\pi i \frac{l}{m}}, \;\; \forall l = 0, 1, \ldots, m-1.$$

Le produit Hermitien s'écrit pour $f_i \in \mathrm{Map}(\mathbb{Z}_m, \mathbb{C})$, $i = 1, 2$:

$$(f_1, f_2) = \sum_{l \in \mathbb{Z}_m} f_1(l) \overline{f_2(l)}.$$

Lemme 4 *Les caractères e forment une base orthogonale de l'espace* $\mathrm{Map}(\mathbb{Z}_m, \mathbb{C})$ *des fonctions à valeurs complexes sur le groupe* $\mathbb{Z}_m$. *On a* $||e||^2 = m$, *ce qui permet de les normaliser.*

Démonstration.

$$\begin{aligned} e_1(l_0)(e_1,e_2) &= \sum_{l\in\mathbb{Z}_m} e_1(l_0)e_1(l)\overline{e_2(l)} \\ &= \sum_{l\in\mathbb{Z}_m} e_1(l_0+l)\overline{e_2(l)} \\ &= \sum_{r\in\mathbb{Z}_m} e_1(r)\overline{e_2(r-l_0)} \\ &= \sum_{r\in\mathbb{Z}_m} e_1(r)\overline{e_2(r)e_2(-l_0)} \\ &= e_2(l_0)(e_1,e_2). \end{aligned}$$

De deux choses l'une : soit $e_1(l_0) = e_2(l_0)$ pour tout l_0, i.e. $e_1 = e_2$, soit $(e_1, e_2) = 0$, i.e. ils sont orthogonaux. Par ailleurs,

$$||e||^2 \,=\, (e,e) \,=\, \sum_{l\in\mathbb{Z}_m} |e(l)|^2 \,=\, m.$$

□

Lemme 5 (Théorème de Plancherel) *Toute fonction $f \in \mathrm{Map}(Z_m, \mathbb{C})$ s'écrit comme "série de Fourier"*

$$f = \sum_{e\in\widehat{Z_m}} \hat{f}(e)e$$

avec comme "coefficients de Fourier"

$$\hat{f}(e) \,=\, \frac{1}{m}(f,e) \,=\, \frac{1}{m}\sum_{l\in\mathbb{Z}_m} f(l)\overline{e(l)},$$

et on a l'identité de Plancherel

$$||f||^2 \,=\, \sum_{l\in\mathbb{Z}_m} |f(l)|^2 \,=\, m\sum_{e\in\widehat{Z_m}} |\hat{f}(e)|^2 \,=\, m||\hat{f}||^2.$$

Démonstration. Pour tout $l_0 \in \mathbb{Z}_m$, on a :

$$\begin{aligned} \sum_{e\in\widehat{Z_m}} \hat{f}(e)e(l_0) &= \sum_{e\in\widehat{Z_m}} e(l_0)\frac{1}{m}\sum_{l\in\mathbb{Z}_m} f(l)\overline{e(l)} \\ &= \sum_{l\in\mathbb{Z}_m} f(l)\frac{1}{m}\sum_{e\in\widehat{Z_m}} e(l_0)\overline{e(l)} \\ &= f(l_0), \end{aligned}$$

où on a utilisé que la somme des exponentielles $\sum_{e\in\widehat{Z_m}} e(l_0)\overline{e(l)}$ est nulle, si $l \neq l_0$, et est égale à m, si $l = l_0$.

Pour la formule de Plancherel, on a d'une part $||f||^2 = \sum_{l\in\mathbb{Z}_m} |f(l)|^2$ par définition. D'une autre part, de $f = \sum_{e\in\widehat{Z_m}} \hat{f}(e)e$, on tire

$$||f||^2 = m \sum_{e\in\widehat{Z_m}} |\hat{f}(e)|^2.$$

En effet,

$$\begin{aligned}
(f,g) &= (\sum_{e\in\widehat{Z_m}} \hat{f}(e)e, \sum_{e'\in\widehat{Z_m}} \hat{g}(e')e') \\
&= m \sum_{e\in\widehat{Z_m}} \hat{f}(e)\overline{\hat{g}(e)},
\end{aligned}$$

et ainsi pour $f = g$: $||f||^2 = m \sum_{e\in\widehat{Z_m}} |\hat{f}(e)|^2$. □

5 Application: algorithme de la TFR

L'algorithme de la TFR (Transformée de Fourier Rapide) est un algorithme récursif pour calculer une transformée de Fourier discrète. Le fait qu'il est récursif permet de réduire le nombre d'opérations.

Ici, on suppose que $m =: N$ est une puissance de 2. La transformée de Fourier discrète F_N associe à un vecteur de n nombres complexes $(u_0, \dots, u_{N-1})$ un vecteur de N nombres complexes $F_N(u_0, \dots, u_{N-1}) = (U_0, \dots, U_{N-1})$ avec

$$U_k = \sum_{j=0}^{N-1} u_j e^{\frac{-2\pi i k j}{N}}.$$

Lemme 6

$$F_N \circ \overline{F_N} = N \text{ id} = \overline{\mathrm{F_N}} \circ \mathrm{F_N}.$$

La démonstration de ce lemme se déduit du fait que $\sum_{k=0}^{N-1} \omega^k = 0$ pour toute racine primitive N-ième de l'unité ω.

On a explicitement:

$$F_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

et

$$F_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}.$$

En réarrangeant l'ordre, on peut écrire:

$$\begin{aligned} U_0 &= u_0 + u_2 + u_1 + u_3 \\ U_1 &= u_0 - u_2 - iu_1 + iu_3 \\ U_2 &= u_0 + u_2 - u_1 - u_3 \\ U_3 &= u_0 - u_2 + iu_1 - iu_3 \end{aligned}$$

ou encore

$$\begin{aligned} \begin{pmatrix} U_0 \\ U_1 \end{pmatrix} &= F_2 \begin{pmatrix} u_0 \\ u_2 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} F_2 \begin{pmatrix} u_1 \\ u_3 \end{pmatrix} \\ \begin{pmatrix} U_2 \\ U_3 \end{pmatrix} &= F_2 \begin{pmatrix} u_0 \\ u_2 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} F_2 \begin{pmatrix} u_1 \\ u_3 \end{pmatrix}. \end{aligned}$$

Ceci sont les formules pour l'algorithme avec *entrelacement temporel*. Les u_j dépendent du temps discret j : dans l'algorithme avec entrelacement temporel, on mélange les temps j qui interviennent.

Sinon, on peut écrire

$$\begin{aligned} U_0 &= u_0 + u_2 + u_1 + u_3 \\ U_2 &= u_0 - u_1 + u_2 - u_3 \\ U_1 &= u_0 - iu_1 - u_2 + iu_3 \\ U_3 &= u_0 + iu_1 - u_2 - iu_3 \end{aligned}$$

ce qui mène ensuite à

$$\begin{aligned} \begin{pmatrix} U_0 \\ U_2 \end{pmatrix} &= F_2 \left[\begin{pmatrix} u_0 \\ u_1 \end{pmatrix} + \begin{pmatrix} u_2 \\ u_3 \end{pmatrix} \right], \\ \begin{pmatrix} U_1 \\ U_3 \end{pmatrix} &= F_2 \left[\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} u_0 - u_2 \\ u_1 - u_3 \end{pmatrix} \right]. \end{aligned}$$

Ceci sont les formules pour l'algorithme avec *entrelacement fréquentiel*. Au lieu de mélanger les différents temps, on mélange les fréquences U_k.

L'algorithme obtient sa récursivité en posant $N = 2M$ et en écrivant:

$$\begin{pmatrix} U_{\text{pair}} \\ U_{\text{impair}} \end{pmatrix} = \begin{pmatrix} F_M & 0 \\ 0 & F_M \end{pmatrix} \begin{pmatrix} I_M & 0 \\ 0 & P_M \end{pmatrix} \begin{pmatrix} u_I + u_{II} \\ u_I - u_{II} \end{pmatrix},$$

où P_M est la matrice diagonale avec $(P_M)_{jj} = e^{\frac{-i\pi j}{M}}$, $u_I = (u_0 u_1 \dots u_{M-1})^t$ et $u_{II} = (u_M u_{M+1} \dots u_{N-1})^t$. On trouve donc

$$F_N u = P \begin{pmatrix} F_{N/2} & 0 \\ 0 & F_{N/2} \end{pmatrix} \begin{pmatrix} I_{N/2} & 0 \\ 0 & P_{N/2} \end{pmatrix} \begin{pmatrix} u_I + u_{II} \\ u_I - u_{II} \end{pmatrix},$$

où P est une matrice de permutations. Le nombre d'opérations (réelles) est égale à $5N \log_2 N$, i.e. de l'ordre de $N \log_2 N$ au lieu de N^2.

6 Caractères

Définition 4
Soit G un groupe, V une représentation de G de dimension finie. Le *caractère* de V est la fonction $\chi_V : G \to \mathbb{C}$ donnée par

$$\chi_V(g) := tr(g|_V),$$

i.e. la trace de l'endomorphisme $\rho(g) \in \mathrm{End}(V)$.

Proposition 3

1. *$\chi_V(hgh^{-1}) = \chi_V(g)$ pour tous $g, h \in G$. En particulier, χ_V est constant sur les classes de conjugaison de G, i.e. χ_v est une* fonction de classe*.*
2. *$\chi_V(1) = \dim V$.*
3. *$\chi_{V \oplus W} = \chi_V + \chi_W$.*
4. *Si G est un groupe fini abélien et V irréductible, χ_V est un homomorphisme de G vers S^1, i.e. on retrouve la définition précédente de caractère comme élément du groupe dual.*

Démonstration.

1. On peut remarquer qu'il est équivalent pour $f \in \mathrm{Map}(G, \mathbb{C})$ d'être une fonction de classe, i.e. pour tous $g, h \in G$: $f(hgh^{-1}) = f(g)$, ou d'être une fonction *centrale*, i.e. pour tous $g, h \in G$: $f(hg) = f(gh)$. La trace vérifie évidement ces conditions.
2. C'est évident.
3. Se montre en choisissant la bonne base dans la somme directe.
4. Ici, on utilise que les représentations irréductibles de groupes abéliens sont de dimension 1. On observe que pour une représentation de dimension 1, déterminant et trace coïncident.

$\square$

Lemme 7 *Soit V une représentation de permutation associée à l'action de G sur un ensemble fini X. Alors $\chi_V(g)$ s'identifie au nombre de points fixes de g.*

Démonstration. Il suffit de décomposer la permutation associée à g en produit de cycles disjoints. Pour chaque l-cycle avec $l > 1$, la matrice est de la forme

$$\begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix},$$

donc la trace est nulle. $\square$

La table des caractères de S_3

On dresse la table des caractères en notant les valeurs que les caractères associés aux différentes représentations irréductibles prennent sur des représentants des classes de conjugaison du groupe. Au-dessus de chaque représentant d'une classe de conjugaison, on note l'effectif de sa classe.

effectif de la classe	1	3	2
représentant de la classe	1	(12)	(123)
triviale U	1	1	1
signature U'	1	-1	1
standard V	2	0	-1

Comment trouve-t-on le caractère de la représentation standard $V = \{ae_1 + be_2 + ce_3 \,|\, a+b+c=0\}$ de S_3 ?

On décompose $\mathbb{C}^3 = U \oplus V$ suivant le sous-espace stable $W = \mathbb{C}(e_1+e_2+e_3)$ qui donne une représentation triviale U, et le caractère de $\mathbb{C}^3$ se trouve à l'aide du Lemme 7 : (3,1,0) est le vecteur des nombres de points fixes sous l'action de chaque représentant sur $\mathbb{C}^3$. Ensuite, $\chi_{\mathbb{C}^3} = \chi_U + \chi_V$, donc

$$\begin{aligned} \chi_V = \chi_{\mathbb{C}^3} - \chi_U &= (3,1,0) - (1,1,1) \\ &= (2,0,-1). \end{aligned}$$

7 La première formule de projection

Cherchons le sous-espace d'une représentation V qui est somme directe de représentations triviales :

$$V^G := \{v \in V \,|\, g \cdot v = v \;\; \forall g \in G\}.$$

Proposition 4 *L'application linéaire*

$$\mathrm{pr} := \frac{1}{|G|} \sum_{g \in G} g|_V$$

(somme des endomorphismes $g|_V$ de V obtenus par les éléments de G) est une projection de V sur V^G.

Démonstration. Soit $v = \mathrm{pr}(w) = \frac{1}{|G|} \sum_{g \in G} g \cdot w$. Alors pour tout $h \in G$,

$$h \cdot v = \frac{1}{|G|} \sum_{g \in G} hg \cdot w = \frac{1}{|G|} \sum_{g \in G} g \cdot w = v,$$

donc $\mathrm{im}(\mathrm{pr}) \subset V^G$. Réciproquement, si $v \in V^G$,

$$\mathrm{pr}(v) \;=\; \frac{1}{|G|}\sum_{g\in G} v \;=\; v,$$

donc $V^G \subset \mathrm{im}(\mathrm{pr})$, et on voit aussi $\mathrm{pr}^2 = \mathrm{pr}$. □

Corollaire 3 *La multiplicité m de la représentation triviale comme sous-représentation d'une représentation V, est donnée par*

$$m \;=\; \dim V^G \;=\; tr(\mathrm{pr}) \;=\; \frac{1}{|G|}\sum_{g\in G}\chi_V(g).$$

En particulier, si V est irréductible et non-triviale, alors la somme des caractères est nulle.

Démonstration. La seule chose à montrer est que la dimension d'un sous-espace s'obtient par la trace de la projection sur ce sous-espace. Or, cela est clair en prenant une base de V, prolongeant une base du sous-espace. Dans une telle base, la matrice de la projection est une matrice diagonale avec des 0 et des 1 sur la diagonale : il y a autant de 1 que la dimension du sous-espace. □

Lemme 8 *Si V, W sont des G-modules, alors* $\mathrm{Hom}(V,W)$ *devient un G-module en posant pour tout $f \in \mathrm{Hom}(V,W)$, tout $g \in G$ et tout $v \in V$:*

$$(g\cdot f)(v) \;:=\; g\cdot f(g^{-1}\cdot v).$$

Si on note $\mathrm{Hom}_G(V,W)$ *l'ensemble des morphismes de G-modules, alors on a pour cette action de G sur* $\mathrm{Hom}(V,W)$*:*

$$\mathrm{Hom}_G(V,W) \;=\; \mathrm{Hom}(V,W)^G.$$

De plus, on a

$$\chi_{\mathrm{Hom}(V,W)} \;=\; \overline{\chi_V}\chi_W.$$

Démonstration. Observons que pour tout $g \in G$, l'endomorphisme $g|_V$ est diagonalisable. En effet, $g|_V$ vérifie l'équation $g^n = 1$ (où n est l'ordre du groupe), et le polynôme $X^n - 1$ est scindé sur $\mathbb{C}$ et à racines simples.

Observons de plus que si λ est valeur propre de $g|_V$, alors $\bar\lambda$ est valeur propre de $g^{-1}|_V$, car les valeurs propres sont des racines de l'unité.

Un $f \in \mathrm{Hom}(V,W)$ est entièrement déterminé par ses coefficients a_{ij} par rapport à une base de l'espace de départ et une de l'espace d'arrivée. On prendra ces bases propres par rapport à l'action de g. Alors $a_{ij} = \mu_j\overline{\lambda_i}$ est la *diagonale* de la matrice, et $\sum_{ij} a_{ij} = \sum_{ij}\mu_j\overline{\lambda_i}$ en est la trace. On trouve bien

$$\sum_{ij}\mu_j\overline{\lambda_i} \;=\; (\mu_1+\ldots+\mu_k)(\overline{\lambda_1}+\ldots+\overline{\lambda_l}).$$

□

Corollaire 4 *Soient V et W deux représentations irréductibles complexes d'un groupe fini G. Alors*

$$\frac{1}{|G|}\sum_{g\in G}\overline{\chi_V(g)}\chi_W(g) \;=\; \left\{\begin{array}{lll} 1 & \textit{si} & V\cong W \\ 0 & \textit{sinon} & \end{array}\right. .$$

Démonstration. Prenons d'abord deux représentations quelconque V et W. Par ce qui précède et le Lemme de Schur, si V est irréductible, $\dim \mathrm{Hom}_G(V,W)$ est la multiplicité de V dans W. De même, si W est irréductible, $\dim \mathrm{Hom}_G(V,W)$ est la multiplicité de W dans V. Maintenant, si V et W sont toutes les deux irréductibles, on a

$$\dim \mathrm{Hom}_G(V,W) \;=\; \left\{\begin{array}{lll} 1 & \textit{si} & V\cong W \\ 0 & \textit{sinon} & \end{array}\right. .$$

En appliquant le Lemme 8 et la formule du Corollaire 3, on obtient bien la formule voulue. □

Définition 5
Soit $\mathbb{C}_{\text{classes}}(G)$ l'ensemble des fonctions de classes sur G, i.e. constantes sur les classes de conjugaison. On pose pour $\alpha,\beta\in\mathbb{C}_{\text{classes}}(G)$

$$(\alpha,\beta) \;:=\; \frac{1}{|G|}\sum_{g\in G}\overline{\alpha(g)}\beta(g).$$

Le corollaire précédent peut aussi se reformuler ainsi:

Théorème 3 *Les caractères de représentations irréductibles forment un système orthonormal pour ce produit Hermitien.*

Consequences:

1. Le nombre de représentations irréductibles est plus petit ou égal au nombre de classes de conjugaison.
2. Toute représentation est déterminée à isomorphisme près par son caractère.
3. V irréductible $\Longleftrightarrow (\chi_V,\chi_V)=1$.
4. La multiplicité a_i d'une représentation irréductible V_i dans une représentation quelconque V est égale à (χ_V,χ_{V_i}).

Démonstration. 1. On remarque que $\dim \mathbb{C}_{\text{classes}}(G)$ est égale au nombre des classes de conjugaison de G.
2. $V\cong V_1^{\oplus a_1}\oplus\ldots\oplus V_l^{\oplus a_l}$ implique $\chi_V=a_1\chi_{V_1}+\ldots+a_l\chi_{V_l}$ et les χ_{V_i} sont linéairement indépendant.

3. $(\chi_V, \chi_V) = \sum_i a_i^2$. $\square$

On obtient plus de conséquences en appliquant tout ceci à la *représentation régulière:*

$$R = \mathbb{C}(G) = \bigoplus_{g \in G} \mathbb{C}e_g.$$

C'est une représentation de permutation, donc le lemme 7 implique que

$$\chi_R(g) = \begin{cases} 0 & si \quad g \neq 1 \\ |G| & si \quad g = 1 \end{cases}.$$

On en déduit que R n'est pas irréductible : si $R = \bigoplus_i V_i^{\oplus a_i}$ avec V_i irréductibles distincts, on a

$$a_i = (\chi_{V_i}, \chi_R) = \frac{1}{|G|}\chi_{V_i}(1)|G| = \dim V_i.$$

D'où

Corollaire 5 *Toute (type d'isomorphie de) représentation irréductible apparaît dans R avec sa dimension* $\dim V_i$ *comme multiplicité.*

Ceci montre encore une fois qu'il n'existe qu'un nombre fini de représentations irréductibles (d'un groupe fini). On a les formules:

$$|G| = \dim R = \sum_i (\dim V_i)^2$$

où la somme s'étend sur un système de représentants des représentations irréductibles, et en appliquant le caractère de R à un élément $g \in G$, $g \neq 1$,

$$0 = \sum_i (\dim V_i)\chi_{V_i}(g).$$

Ces formules permettent très souvent de connaître le caractère manquant quand on a déterminé tous les caractères sauf un.

8 Plus de formules de projection

but: Montrer que les caractères forment une base dans l'espace des fonctions de classes, et donc que le nombre de représentations irréductibles de G égale le nombre de classes de conjugaison.

question de départ: Quelles combinaisons linéaires des endomorphismes $g : V \to V$ sont des G-morphismes ?

Proposition 5 *Soit $\alpha : G \to \mathbb{C}$ une application quelconque. Posons pour toute G-représentation V :*

$$\phi_{\alpha,V} := \sum_{g \in G} \alpha(g) g \, : \, V \to V.$$

Alors $\phi_{\alpha,V}$ est un G-morphisme pour tout V si et seulement si α est constante sur les classes de conjugaison.

Démonstration. Soient $h \in G$ et $v \in V$. Si α est une fonction de classes, alors

$$\begin{aligned}
\phi_{\alpha,V}(h \cdot v) &= \sum_{g \in G} \alpha(g) g \cdot (h \cdot v) \\
&= \sum_{hgh^{-1} \in G} \alpha(hgh^{-1}) hgh^{-1} \cdot (h \cdot v) \\
&= h \cdot \left(\sum_{hgh^{-1} \in G} \alpha(hgh^{-1}) g \cdot v \right) \\
&= h \cdot \left(\sum_{hgh^{-1} \in G} \alpha(g) g \cdot v \right) \\
&= h \cdot \phi_{\alpha,V}(v).
\end{aligned}$$

Réciproquement, si α n'est pas une fonction de classes, il existe une représentation V pour laquelle $\phi_{\alpha,V}$ n'est pas un G-morphisme. En effet, prenons $V = R$ la représentation régulière. $R = \bigoplus_{g \in G} \mathbb{C} e_g$. Il existe g et $h^{-1}gh \in G$ avec $\alpha(g) \neq \alpha(h^{-1}gh)$. Si on avait

$$\phi_{\alpha,R}(h \cdot e_l) = h \cdot \phi_{\alpha,R}(e_l),$$

alors d'une part

$$\sum_{k \in G} \alpha(k) k \cdot (h \cdot e_l) = \sum_{k \in G} \alpha(k) e_{khl},$$

et d'une autre part

$$h \cdot \left(\sum_{\tilde{k} \in G} \alpha(\tilde{k}) \tilde{k} \cdot e_l \right) = \sum_{\tilde{k} \in G} \alpha(\tilde{k}) e_{h\tilde{k}l} = \sum_{k \in G} \alpha(h^{-1}kh) e_{khl},$$

en choisissant $\tilde{k} = h^{-1}kh$. En particulier, pour $k = g$, on compare le coefficient devant e_{ghl} et on obtient $\alpha(g) \neq \alpha(h^{-1}gh)$. Ceci est une contradiction qui montre finalement notre affirmation. □

Proposition 6 *Le nombre de représentations irréductibles d'un groupe fini G est égal au nombre de classes de conjugaison de G.*

De façon équivalente, les caractères de représentations irréductibles forment une base orthonormée de $\mathbb{C}_{\text{classes}}(G)$.

Démonstration. Soit $\alpha \in \mathbb{C}_{\text{classes}}(G)$ avec $(\alpha, \chi_V) = 0$ pour toute représentation irréductible V. Il faut montrer $\alpha = 0$.

Soit $\phi_{\alpha,V} = \sum_{g \in G} \alpha(g) g : V \to V$ comme ci-dessus. Par le Lemme de Schur, $\phi_{\alpha,V} = \lambda \mathrm{id_V}$. Supposons $n = \dim V$, alors

$$\begin{aligned}
\lambda &= \frac{1}{n} tr(\phi_{\alpha,V}) \\
&= \frac{1}{n} \sum_{g \in G} \alpha(g) \chi_V(g) \\
&= \frac{|G|}{n} \overline{(\alpha, \chi_{V^*})} \\
&= 0,
\end{aligned}$$

où on a utilisé la représentation duale $V^* = \mathrm{Hom}(V, \mathbb{C})$ de V, définie par

$$\rho_{V^*}(g) = {}^t\rho_V(g^{-1}) : V^* \to V^*,$$

pour tout $g \in G$. On a bien $\chi_{V^*} = \overline{\chi_V}$.

Ainsi, on conclut que $\phi_{\alpha,V} = 0$ pour toute représentation irréductible V. Or, toute représentation est somme de représentations irréductibles, donc $\phi_{\alpha,V} = 0$ pour toute représentation V. Ceci est donc en particulier vrai pour la représentation régulière R. Mais pour R, les e_g pour $g \in G$ sont linéairement indépendants, donc $(\sum_{g \in G} \alpha(g) g)(e_1) = \sum_{g \in G} \alpha(g) e_g$ est une combinaison linéaire d'éléments d'une base, et par suite $\alpha(g) = 0$ pour tout $g \in G$. $\square$

Références: J'ai pris la plupart des démonstrations dans le livre de J. Harris et W. Fulton, Representation theory, (Springer 2004) qui est remarquablement bien écrit. Sinon, le livre de J.-P. Serre, Représentations linéaires des groupes finis, (Hermann 1998) est une référence classique en Français. Une autre référence en Français est le livre de G. Rauch, Les groupes finis et leurs représentations, (Ellipse 2000).

Pour la partie sur les groupes abéliens, j'ai utilisé le livre de H. Dym et H. P. McKean, Fourier series and integrals (Academic Press 1972). J'ai pris la transformée de Fourier rapide dans le livre de M. Schatzman, Analyse numérique (Dunod 2004).